

CLAIMS

1. A network security system, comprising a firewall arranged between an internal network and an external network, said firewall comprises
5 a first port configured at the internal network oriented side of the firewall and a second port configured at the external network oriented side of the firewall; wherein

the network security system further comprises a trusted node arranged between the firewall and the external network, which is used
10 to provide a data channel between the internal network and external network, and forward the data transported between the internal network and external network; and the trusted node comprises a media-stream receiving port used to converge the data from the second port.

15 2. The network security system according to claim 1, wherein

the trusted node further comprises a data forward unit, which is used to forward the data transported between the internal network and the external network, a signaling channel selection unit, which
20 is used to select signaling transmission channel for transmitting the data so as to implement the convergence of signaling, a call channel selection unit, which is used to select a media-stream receiving port in the trusted node for communicating with the internal network, and a control unit, which is used to control the
25 operations of all the other units.

3. The network security system according to claim 1 or 2, wherein the trusted node is designed to support H.323 protocol.

4. The network security system according to claim 1 or 2, wherein the signaling channel selection unit adopts Q931 channel for transmitting signaling.

5 5. A network security method of realizing secure communication between the internal network and the external network by utilizing a network security system, said network security system comprises a firewall arranged between the internal network and the external network, a first port and a second port configured at the both sides
10 of the firewall, and a trusted node arranged between the firewall and the external network; and the trusted node comprises a media-stream receiving port; wherein the network security method comprises the following steps of:

A. establishing a call connection between the internal network
15 and the external network by means of the trusted node;

B. selecting a media-stream receiving port for communicating with the internal network in the trusted node;

C. the trusted node forwarding the data transported between the internal network and the external network, and at the same time,
20 converging the data from the second port by the selected media-stream receiving port.

6. The network security method according to claim 5, wherein the Step B comprises the following:

25 B1. Open Logical Channel signaling being transmitted by the internal network to the trusted node;

B2. the trusted node informing the internal network of the selected media-stream receiving port;

B3. the trusted node transmitting Open Logical Channel signaling

to the external network to establish a corresponding channel.

7. The network security method according to claim 5, wherein the Step C comprises the following:

5 C1. the selected media-stream receiving port of the trusted node receiving all the data from the internal network, and forwarding the data to the external network;

C2. the selected media-stream receiving port of the trusted node forwarding the data transmitted by the external network to the
10 internal network.

8. The network security method according to claim 5, wherein the Step A comprises a step of selecting Q931 channel for transmitting signaling.

15

9. The network security method according to of any one of claim 5 to 8,

further comprises a step of implementing load balance among a plurality of trusted nodes when the data are forwarded.